WE CLAIM AS OUR INVENTION:

Sub a1

1. A method for protecting a security module, in which security-relevant data are stored, inserted on a device motherboard, comprising the steps of:

monitoring proper insertion of said security module on said device motherboard with a first function unit, a second function unit and a third function unit in said security module;

detecting at least one of improper use and improper replacement of said security module with said second function unit and, upon a detection of at least one of said improper use and said improper replacement, said second function unit causing said security-relevant data to be erased;

during replacement of said security module, inhibiting functioning of said security module with said third function unit;

following at least one of proper use and proper replacement of said security module, re-initializing, with said first function unit, any erased, security-relevant data; and

after said re-initializing, enabling each of said first function unit, said second function unit and said third function unit to re-commission said security module.

2. A method as claimed in claim 1 wherein the step of re-initializing comprises determining at least one of said proper use and proper replacement of said security module by establishing communication between said first function unit and a remote data source exchanging information between said first function unit and said

remote data source via current loop, and detecting that at least one of said proper use and proper replacement has occurred if said exchange of data takes place error-free.

3. A security module for insertion on a device motherboard, comprising:

a memory in which security-relevant data are stored;

a voltage monitoring unit which supplies an operating voltage to said memory to maintain said security-relevant data stored therein and which disconnects said memory from said voltage, thereby erasing said security-relevant data therein, upon occurrence of a voltage level indicating at least one of improper use and replacement;

an unplugged status detection unit which inhibits functioning of said security module during replacement of said security module and which has a self-holding capability, indicating that said security module has been replaced, which is triggered when a voltage level a test voltage line deviates from a predetermined voltage level; and

a processor connected to said voltage monitoring unit and to said unplugged status detection unit to re-commission said security module after at least one of said improper use and replacement, by enabling said voltage monitoring unit and said unplugged status detection unit, including resetting said unplugged status detection unit.

4. A security module as claimed in claim 3 wherein said unplugged status detection unit comprises a line and switch element for resetting said self-holding

capability, said switch element being triggered by a signal from said processor on said line.

5. A security module as claimed in claim 4 wherein said unplugged status detection unit comprises:

a voltage divider comprising a series resistor circuit connected across a terminal for receiving a supply voltage, tapped by a capacitor, and a line having a test voltage thereon;

a diode connected between said terminal for receiving a supply voltage and said capacitor;

a comparator having a non-inverting input, an inverting input connected to a reference voltage source, and a comparator output;

a further capacitor tapping said voltage divider and connected to said non-inverting input of said comparator;

said comparator output being connected to a line at a voltage potential via an inverter;

a switch element having a control input connected to said comparator output, said switch element producing said self-holding capability and being connected in parallel with a resistor of said voltage divider; and

said switch element for resetting said self-holding capability being connected between said voltage divider tap for said further capacitor, and ground.

6. A security module as claimed in claim 5 further comprising an interrogation line connected between said processor and said unplugged status detection unit for interrogating a self-holding status of said unplugged status detection unit by said processor.

7. A security module as claimed in claim 6 wherein said line having said test voltage thereon is at ground potential, and wherein said line at a voltage potential connected to said comparator output is at operating voltage potential when said security module is plugged into said device motherboard and is otherwise at ground potential when said security module is not plugged into said device motherboard.

8. A security module as claimed in claim 3 wherein said memory is contained in said processor and is at an operating voltage supplied from said voltage monitoring unit as long as said processor is supplied with system voltage, and wherein said processor has a terminal for resetting said self-holding capability of said unplugged status detection unit, and a further terminal for interrogating a status of said unplugged status detection unit.

9. A security module as claimed in claim 8 further comprising an ASIC connected to said processor via an internal data bus, said ASIC having a first contact group for connection to a system bus of a device containing said device motherboard.

10. A security module as claimed in claim 3 further comprising a printed circuit board on which said processor, said voltage monitoring circuit and said unplugged status detection unit are mechanically and electrically mounted, said printed circuit board having contact terminals for a battery;

a security module housing formed by a hard casting compound surrounding said printed circuit board and said processor, said voltage monitoring circuit and said unplugged status detection circuit thereon, with said contact terminals being exposed to an exterior of said housing;

a battery replaceably connected to said contact terminals outside of said housing; and

said printed circuit board having a first contact group, accessible from outside of said housing, for communicating with a system bus of a device containing said device motherboard, and a second contact group accessible from an exterior of said housing for receiving system voltage, and at least one of said first contact group and said second contact group being connected to said unplugged status detection unit to monitor a plugged status of said security module.

11. A security module as claimed in claim 10 wherein said processor includes terminals for monitoring said plugged status of said security module with lines forming a current loop when said security module is plugged into said device motherboard.

12. A security module as claimed in claim 3 wherein said processor has a terminal for emitting at least one signal identifying a status of said security module.

13. A security module as claimed in claim 12 wherein said processor is connected to an input/output unit having input/output ports, and having at least one internal signaling element in said security module connected to said input/output ports.